Re

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,683	02/08/2002	Nir Zuk	ONS-001	2532

44987 7590 04/05/2006

HARRITY SNYDER, LLP
11350 Random Hills Road
SUITE 600
FAIRFAX, VA 22030

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/072,683	ZUK ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-69* is/are pending in the application.

4a) Of the above claim(s) *20,30,34 and 36* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19,21-29,31-33,35 and 37-69* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated January 20, 2006 with the amendments to claims 1, 3, 5, 9, 17-19, 21, 22, 24, 27, 29, 31, 33, 37, 39, 40, 42-44, 46, 49, 52, 57, 59 and 65-67 and the cancellation of claims 20, 30, 34 and 36.

2. Claims 1-19, 21-29, 31-33, 35 and 37-69 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-19, 21-29, 31-33, 35 and 37-69 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 18, 27 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: what is the connection of the step of grouping the plurality of TCP packets into packet flows and sessions, wherein grouping the plurality of TCP packets into packet flows and sessions

comprises string the packet flows and sessions in a hash table, with a method for detecting and preventing security breaches in a network.

Claim Objections

6. Claim 17 is objected to because of the following informalities: "attack signatures signature". Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-7, 12-17, 21-25, 31, 33, 35, 37-40, 43-45, 49-50, 52-55, 58, 60 and 63-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) and Gleichauf et al. (6,324,656) in view of Nikander et al. (6,253,321).

a) As to claims 1 and 24, Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly discloses this limitation (i.e. TCP stream reassembly) (col. 6, lines 39-40), to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to

each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of a security breach (col. 3, lines 1-4), wherein inspecting the TCP stream to detect information indicative of a security breach (col. 2, lines 50-55) comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (col. 6, lines 31-33; col. 8, lines 20-35).

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (Fig. 3B; col. 6, lines 32 – col. 7, line 5).

Gleichauf does not explicitly disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches.

Nikander is relied on for the teaching of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and

forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

b) As to claims 2, 12 and 15, Gleichauf discloses inspecting the TCP stream to detect information indicative of security breaches comprising inspecting the TCP stream for protocol irregularities (col. 6, lines 36-42).

c) As to claims 3, 13, and 16-17, Gleichauf discloses inspecting the TCP to detect information indicative of a security breach comprising searching the TCP stream for attack signatures (col. 1, lines 29-31).

d) As to claims 4, 31, 35, 50, 54, 66 and 69, Gleichauf discloses searching the TCP stream for attack signatures comprises using stateful signature detection (col. 6, lines 45-52).

e) As to claims 5, 14, 33, 52 and 67, Gleichauf discloses inspecting the TCP stream to detect information indicative of a security breach using a plurality of network intrusion detection methods (col. 6, lines 66-67).

f) As to claims 6, 49, 53, 65 and 68, Gleichauf discloses the plurality of network intrusion detection methods comprises at least protocol anomaly detection (col. 6, lines 36-42).

g) As to claim 7, Gleichauf discloses the plurality of network intrusion detection methods comprises at least signature detection (col. 6, lines 43-45).

h) As to claims 21 and 38, Gleichauf discloses searching the TCP stream for attack signatures comprises querying the signatures database to determine whether there are matching signatures in the TCP stream (col. 6, lines 45-52; col. 5, lines 36-42).

i) As to claims 22 and 39, Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly discloses this limitation (i.e. TCP stream reassembly) (col. 6, lines 39-40), to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of a security breach (col. 3, lines 1-4), querying a signatures database to determine whether there are matching signatures in the TCP stream (col. 6, lines 45-52; col. 5, lines 36-42).

Gleichauf does not explicitly disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches.

Nikander is relied on for the teaching of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf and Nikander do not expressly disclose using deterministic finite automata for pattern matching when querying a signatures database to determine whether there are matching signatures in the TCP stream.

The examiner takes official notice that use of deterministic finite automaton for providing a pattern matching is well known in the theory of computation.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of deterministic finite automaton for providing a pattern

matching is well known in the theory of computation in the system of Gleichauf and Nikander so as to effectively implementing pattern matching.

j) As to claims 23, 25, 45 and 58, Gleichauf discloses reconstructing the plurality of TCP packets from a plurality of packet fragments (col. 6, lines 39-40).

k) As to claim 37, Gleichauf (6,324,656) discloses the protocol specifications comprise specifications of one or more of TCP protocol, HTTP protocol, SMTP protocol, FTP protocol, NETBIOS protocol, IMAP protocol, POP3 protocol, TELNET protocol, IRC protocol, RSH protocol, REXEC protocol, and RCMD protocol (Fig. 3B).

l) As to claims 40, 55, 60 and 63-64, Gleichauf discloses a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream (col. 7, lines 1-5); a routine for storing a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented (col. 5, lines 33-42); a routine for distributing the network security policy to one or more gateway points in the network (Fig. 2, element 20) and a routine for updating the protocol database and the signatures database (col. 9, lines 7-13).

m) As to claim 43, Gleichauf discloses the network intrusion detection and prevention sensor is placed inside a firewall (col. 4, lines 47-49).

n) As to claim 44, Gleichauf discloses the network intrusion detection and prevention sensor is placed outside a firewall (col. 5, lines 24-27).

9. Claims 8-11, 18, 26-28, 32, 41, 47-48, 51, 56 and 61-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) and Gleichauf et al. (6,324,656) in view of Nikander et al. (6,253,321) and further in view of Copeland, III (2003/0105976).

a) As to claims 8, 26 and 47, Gleichauf and Nikander do not disclose grouping the plurality of TCP packets into packet flows and sessions.

Copeland discloses a flow-based intrusion detection system for detecting intrusions in computer communication networks comprising grouping the plurality of TCP packets into packet flows and sessions (Fig. 1, elements "FLOW F1-FLOW F4"; page 5, paragraph [0058]; Fig. 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions in the system of Gleichauf and Nikander, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

b) As to claims 9, 28 and 48, Copeland discloses storing the packet flows in packet flow descriptors (page 5, paragraph [0059-0061]).

c) As to claims 10-11, Copeland discloses searching the packet flow descriptors for traffic signatures and inspecting the TCP stream comprises searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream (page 6, paragraph [0070]).

d) As to claims 18 and 27, Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly discloses this limitation (i.e. TCP stream reassembly) (col. 6, lines 39-40), to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of a security breach (col. 3, lines 1-4).

Gleichauf does not explicitly disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches.

Nikander is relied on for the teaching of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of security breaches (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP

packet to a network destination if the TCP stream does not contain information indicative of security breaches in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf and Nikander do not expressly disclose grouping the plurality of TCP packets into packet flows and sessions, wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table.

Copeland discloses a flow-based intrusion detection system for detecting intrusions in computer communication networks comprising grouping the plurality of TCP packets into packet flows and sessions (Fig. 1, elements "FLOW F1-FLOW F4"; page 5, paragraph [0058]; Fig. 3), wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table (page page 9, paragraph [0107]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of grouping the plurality of TCP packets into packet flows and sessions, wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table in the system of Gleichauf and Nikander, as Copeland teaches so as to effectively determine if the traffic data appears to be legitimate or possible suspicious activity.

d) As to claims 32 and 51, Copeland discloses a traffic signature detection software module for searching the packet flow descriptors for traffic signatures (page 4, paragraphs [0047-0051]).

e) As to claims 41, 56, and 61-62, Copeland discloses the system further comprising a graphical user interface comprising a routine for displaying network security information to network security administrators; and a routine for specifying a network security policy (page 11, paragraph [0182]).

10. Claims 19 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) and Gleichauf et al. (6,324,656) in view of Nikander et al. (6,253,321) in view of Copeland, III (2003/0105976) and further in view of Alexander et al. (2004/0258073).

Gleichauf, Nikander and Copeland do not expressly disclose computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type.

Alexander discloses computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type (page 3, paragraph [0027]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of computing a hash value from a 5-tuple comprising a source IP address, a destination IP address, a source port, a destination port and a protocol type in the system of Gleichauf, Nikander and Copeland as Alexander teaches so as to effectively performing packet filtering.

11. Claims 42, 46, 57 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf et al. (6,499,107) in view of Nikander et al. (6,253,321) and further in view of Trcka et al. (6,453,345).

a) As to claims 42 and 57, Gleichauf discloses a method and system for adaptive network security using intelligent packet analysis comprising reassembling a plurality of TCP packets in the network traffic into a TCP stream, Gleichauf implicitly discloses this limitation (i.e. TCP stream reassembly) on col. 6, lines 39-40, to make it even clearer, the examiner takes official notice that use of reassembling TCP packets into a TCP stream is quite well known in data communications network. Data traveling over an IP network is always broken up into packets, the IP protocol adds information to each packet so that the routers along the network know where the data came and where it is going, the packets may be received out of order, or not, and are reassembled in the proper order at the destination computer; inspecting the TCP stream to detect information indicative of security breaches (col. 3, lines 1-4), wherein inspecting the TCP stream to detect information indicative of a security breach (col. 2, lines 50-55) comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (col. 6, lines 31-33; col. 8, lines 20-35).

Gleichauf (6,324,656) also discloses inspecting the TCP stream to detect information indicative of a security breach comprises storing a plurality of protocol specifications supported by the network in a protocol database; and querying the

protocol database to determine whether the plurality of TCP packets are compliant with one or more of the plurality of protocol specifications in the protocol database (Fig. 3B; col. 6, lines 32 – col. 7, line 5).

Gleichauf does not disclose dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of a security breach.

Nikander discloses dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of a security breach (col. 4, lines 41-45).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of a security breach and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of a security breach in the system of Gleichauf, as Nikander teaches so as to effectively manage communications data.

Gleichauf and Nikander do not disclose a central management server and a graphical user interface.

Trcka discloses a network security and surveillance system comprising a central management center (col. 15, lines 13-21; Fig. 8, element 64) to control the network

intrusion detection and prevention sensor and a graphical user interface for configuring the network intrusion detection and prevention sensor (col. 13, lines 50-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ to use of having a central management server to control the network intrusion detection and prevention sensor and a graphical user interface for configuring the network intrusion detection and prevention sensor (col. 13, lines 50-65) in the system of Gleichauf and Nikander as Trcka teaches so as to detect and protect against security breaches, network failures and other types of data compromising events (col. 1, lines 10-15).

b) As to claims 46 and 59, Nikander discloses dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches and forwarding a TCP packet to a network destination if the TCP stream does not contain information indicative of a security breach (col. 4, lines 41-45).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
3/31/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER